

日 本 国 特 許 庁
JAPAN PATENT OFFICE

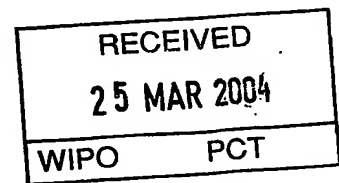
30. 1. 2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 月 3 1 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 0 2 4 1 6 7
Application Number:
[ST. 10/C] : [J P 2 0 0 3 - 0 2 4 1 6 7]



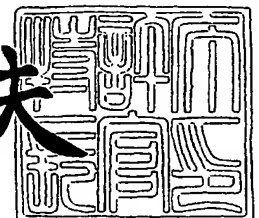
出 願 人 松下電器産業株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 3 月 1 2 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



BEST AVAILABLE COPY

【書類名】 特許願

【整理番号】 2968240067

【提出日】 平成15年 1月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00542
G06K 19/07

【発明者】

【住所又は居所】 東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内

【氏名】 江原 裕美

【発明者】

【住所又は居所】 東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内

【氏名】 川野 眞二

【発明者】

【住所又は居所】 東広島市鏡山3丁目10番18号 株式会社松下電器情報システム広島研究所内

【氏名】 中部 太志

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体メモリカード、コンピュータ読み取り可能なプログラム

【特許請求の範囲】

【請求項 1】 耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記処理部は、

当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う

ことを特徴とする半導体メモリカード。

【請求項 2】 前記処理部は、

使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、

アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)、

アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)暗復号化部を備える

ことを特徴とする請求項 1 記載の半導体メモリカード。

【請求項 3】 前記処理部は、アプリケーションプログラムからセキュリティレベルを受け付ける受付部と、

セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を記憶する記憶部とを備え、

前記暗復号化部により割り当てられる暗号鍵は、

受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成さ

れ、

前記暗復号化部による暗号化及び復号化は、

受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされる

ことを特徴とする請求項 2 記載の半導体メモリカード。

【請求項 4】 前記暗復号化部は、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で耐タンパモジュールの内部メモリ上に配置する

ことを特徴とする請求項 3 記載の半導体メモリカード。

【請求項 5】 前記処理部は、別のアプリケーションプログラムの利用領域の拡張を、

不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアクセステーブルを配置することにより行い、

前記暗復号化部は、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置する

ことを特徴とする請求項 3 記載の半導体メモリカード。

【請求項 6】 耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記処理部は、

当該アプリケーションプログラムに固有のファイルシステム領域と、当該ファイルシステム領域についてのアクセステーブルとを不揮発メモリ上に配置し(1)

、
これらファイルシステム領域及びアクセステーブルのそれぞれに相異なる暗号

鍵を割り当て(2)、

それら相異なる暗号鍵を耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う(3)

ことを特徴とする半導体メモリカード。

【請求項7】 耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードにおいて、耐タンパモジュール内のCPUにより実行されるコンピュータ読取可能なプログラムであって、

耐タンパモジュールは、内部メモリを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張する手順をCPUに行わせる

ことを特徴とするコンピュータ読取可能なプログラム。

【請求項8】 前記コンピュータ読取可能なプログラムは、

使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、

アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)、

アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)手順をCPUに行わせる

ことを特徴とする請求項7記載のコンピュータ読取可能なプログラム。

【請求項9】 前記コンピュータ読取可能なプログラムは、アプリケーションプログラムからセキュリティレベルを受け付ける受付ステップをCPUに実行させるものであり、

耐タンパモジュールの内部メモリには、

セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を示すテーブルが存在し、

前記暗復号化ステップにより割り当てられる暗号鍵は、
受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成され、

前記暗復号化ステップによる暗号化及び復号化は、
受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされる

ことを特徴とする請求項 8 記載のコンピュータ読取可能なプログラム。

【請求項 10】 前記暗復号化ステップは、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で耐タンパモジュールの内部メモリ上に配置する手順を CPU に行わせる

ことを特徴とする請求項 9 記載のコンピュータ読取可能なプログラム。

【請求項 11】 前記コンピュータ読取可能なプログラムは、別のアプリケーションプログラムの利用領域の拡張にあたって、

不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアクセステーブルを配置する処理を CPU に行わせ、

前記暗復号化ステップは、

ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置する手順を CPU に行わせる

ことを特徴とする請求項 9 記載のコンピュータ読取可能なプログラム。

【請求項 12】 耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードにおいて、耐タンパモジュール内の CPU により実行されるコンピュータ読取可能なプログラムであって、

耐タンパモジュールは、内部メモリと、処理部とを含み、

耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、

前記コンピュータ読取可能なプログラムは、

当該アプリケーションプログラムに固有のファイルシステム領域と、当該ファイルシステム領域についてのアクセステーブルとを不揮発メモリ上に配置し(1)

これらファイルシステム領域及びアクセステーブルのそれぞれに相異なる暗号鍵を割り当て(2)、

それら相異なる暗号鍵を耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行う(3)手順をCPUに行わせる

ことを特徴とするコンピュータ読取可能なプログラム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】

本発明は、格納内容のセキュリティを保証した半導体メモリカードに関し、その記憶容量を拡張する技術の改良に関する。

【0002】

【従来の技術】

半導体メモリカードの生産業は、放送・出版等のマスメディアから金融機関、国、自治体まで、様々な分野からの注目を浴びる近年の急成長産業である。

これらの分野から注目を集めているのは、格納内容の保護機能である。格納内容の保護機能をもった半導体メモリカードの代表格は、SDメモリカード、非接触ICカードである。SDメモリカードは、接触型の半導体メモリカードであり、不揮発メモリと、ロジック回路と、コネクタとを備える、コネクタを介してホスト装置が接続した場合、SDメモリカードはチャレンジ・レスポンス型の相互認証を行い、互いの正当性を認識した上で、ホスト装置による不揮発メモリのアクセスを許可する。不正な機器によるアクセスを排斥することができ、また内蔵している不揮発メモリの規模は、64Mバイト～1Gバイトという大規模なものである。SDメモリカードは、著作権保護が必要なオーディオデータ、ビデオデータの格納に向いている。

【0003】

非接触ICカードは、CPU、マスクROM、EEPROMを内蔵したICチップを板体に配してなる。板体には螺旋アンテナが埋設されており、非接触ICカードがこの螺旋アンテナを介して、ホスト装置と非接触型のデータ入出力を行う。またこのICチップは耐タンパモジュールと呼ばれ、分解や解析等のリバース行為に耐性をもつ。

この耐性があるため、非接触ICカードは金銭決済用途に向いており、多くのクレジット会社や金融機関がこの非接触ICカードの採用を検討している。その反面、耐タンパモジュールは、単位面積当たりの製造コストが高く、耐タンパモジュール内のEEPROMの規模は160Kバイト程度である。

【0004】

このようにSDメモ리카ード、非接触ICカードには一長一短があり、どちらが優れているかは簡単には結論付けることはできない。

尚、SDメモ리카ードについての先行技術には、以下の特許文献1に開示されたものがある。

【0005】

【特許文献1】

特開2001-14441号公報

【0006】

【発明が解決しようとする課題】

ところで、クレジット会社のサーバ装置をホスト装置とした電子商取引(EC(Electronic Commerce))では、年間の取引明細をダウンロードして、非接触ICカードに格納しておきたいことがある。年間の取引明細となると、データサイズが大きく、非接触ICカードのメモリでは容量に不足が生じる。容量が不足するとはいえ、SDメモ리카ードのような耐タンパモジュールの無い半導体メモ리카ードに取引明細を格納しようというのは、クレジット会社にとって不安が残る。何故なら、かかる年間の取引明細は、金銭に至らないまでも、それに準ずる保護価値があるからである。

【0007】

半導体メモ리카ードを製造する生産業のメーカは、製造コストの高騰を承知で耐タンパモジュールを大規模するか、或は、クレジット会社の要求を黙殺するか

を選択せざるを得ない。現状では、半導体メモリカードのメーカは苦渋の決断を迫られているといえる。

本発明の目的は、金銭に準ずるデータであってサイズが膨大なものを、相応のセキュリティレベルで格納しておくことができる半導体メモリカードを提供することである。

【0008】

【課題を解決するための手段】

上記目的を達成するため、本発明に係る半導体メモリカードは、耐タンパモジュールと、不揮発メモリとを備え、耐タンパモジュールは、内部メモリと、処理部とを含み、耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、前記処理部は、当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行うことを特徴としている。

【0009】

【発明の実施の形態】

以降、本発明に係る半導体メモリカードの実施形態について説明する。本実施形態に係る半導体メモリカードは、非接触ICカードの耐タンパモジュールを内蔵したSDeXメモリカードである。SDeXメモリカードは、SDメモリカード同様、SDポータブルデバイスの記録媒体に用いられながらも、非接触ICカードの耐タンパモジュールを内蔵している。

【0010】

先ず始めに、本発明に係る半導体メモリカード(SDeXメモリカード)の実施行為のうち、使用行為について説明する。SDeXメモリカードは、携帯電話などのSDポータブルデバイスと接続され、図1に示すような環境で、ユーザの利用に供される。図1は、SDeXメモリカードの使用環境を示す図である。

図1における使用環境は、ECサーバ100、カードリーダーライタ200、無線基地局210、SDポータブルデバイス300から構成される。

【0011】

ECサーバ100は、カードリーダーライタ200及び無線基地局100、ネットワークを介して、非接触ICカードにECサービスを提供する。ECサーバ100には複数のECアプリケーションプログラムが動作しており、これらのそれぞれは、固有のECサービスを非接触ICカードに提供する。ECサーバ100上で動作するECアプリケーションは、サーバアプリケーションであり、ECサービスの種類毎にそれぞれ違うものが存在する。図1では、n種のECサービス毎のECアプリをS_APL1, 2, 3...nと略記している。これらは、n種のサーバアプリケーションである。ECサーバ100によるECサービス提供は、ネットワーク、カードリーダーライタ200及び無線基地局210を介してECコマンドを非接触ICカードに発行することによりなされる。

【0012】

カードリーダーライタ200は、クレジット会社・金融機関のキャッシュデスペンサー、店舗のレジ機に備え付けの機器であり、非接触ICカードへの電力供給、非接触ICカードとの非接触型の入出力を行う。カードリーダーライタ200は、ネットワークと接続されており、このカードリーダーライタ200を介することで、非接触ICカードはECサーバ100のECサービスを受けることができる。

【0013】

無線基地局210は、建造物や電柱の屋上に備え付けの機器であり、携帯電話型のSDポータブルデバイス300と無線によるデータの入出力を行う。無線基地局210は、ネットワークと接続されており、この無線基地局210を介することでも、SDポータブルデバイス300はECサーバ100のECサービスを受けることができる。

【0014】

SDポータブルデバイス300は、SDeXメモリカードを接続して、SDeXメモリカードをアクセスする機器である。SDポータブルデバイス300には、ブラウザソフト等がインストールされており、ユーザはこのブラウザのユーザインターフェイスを介して、SDeXメモリカードにおけるファイルシステム(File System(以下、FSと略す場合がある))をアクセスすることができる。このファイルシステムア

アクセスは、SDメモリカードで規定されているSDコマンドをSDeXメモリカードに発行し、そのレスポンスをSDeXメモリカードから受信することでなされる。また、SDポータブルデバイス 300 がSDeXメモリカードからブートストラップを行って起動する場合、SDポータブルデバイス 300 はSDeXメモリカードと一体になって非接触ICカードとして機能する。SDポータブルデバイス 300 の背面には、螺旋アンテナが埋設されており、非接触ICカードとしての機能時において、この螺旋アンテナが、カードリーダーライタ 200 から発せられる電力をSDeXメモリカードに供給する。またSDポータブルデバイス 300 は、SDeXメモリカードに対するコマンド・レスポンスと、ECサーバ 100 とのコマンド・レスポンスとの相互変換を行う。SDポータブルデバイス 300 による相互変換とは、ECサーバ 100 からのECコマンドをカプセル化した拡張SDコマンドを生成してSDeXメモリカードに出力し、SDeXメモリカードからのSDレスポンスよりECレスポンスを取り出して、ECサーバ 100 に出力する処理である。SDポータブルデバイス 300 がSDeXメモリカードにてブートストラップを行い、非接触ICカードとして機能することを『ECモード』という。また、SDポータブルデバイス 300 がSDeXメモリカードを記録体として用いることを『SDモード』という。

【0015】

SDモードでのSDeXメモリカードの利用は、SDeXメモリカード本来の用途である。この用途においてSDeXメモリカードのホスト装置となるのは、SDポータブルデバイス 300 であり、ホスト装置であるSDポータブルデバイス 300 が配信サーバからダウンロードしたオーディオデータ、ビデオデータの受け皿として、SDeXメモリカードは用いられる。こうしてSDeXメモリカードに記録されたオーディオデータ、ビデオデータをホスト装置は再生させることができる。

【0016】

ECモードでのSDeXメモリカードの利用は、非接触ICカードの用途である。このECモードにおいてもSDeXメモリカードはSDポータブルデバイス 300 と接続される。しかしSDeXメモリカードのホスト装置となるのはこのSDポータブルデバイス 300 ではなく、ネットワーク上のECサーバ 100 である。SDeXメモリカードと接続されたSDポータブルデバイス 300 を、カードリーダーライタ 200、無線基

地局 210 と用いることにより、SDeX メモリカードは EC サーバ 100 と通信を行う。この通信により、EC サーバ 100 と金銭決済を行うことができる。

【0017】

本実施形態の SDeX メモリカードは、配信されたオーディオデータ、ビデオデータの受け皿としても用途に加え、非接触 IC カードとしても用途が存在するので、ユーザにとっての利便性が増している。

尚図 1 において SDeX メモリカードは、SD モードにおいてカードリーダー 200 を介して、EC サーバ 100 をアクセスしたが、無線基地局 210 を介して SD ポータブルデバイス 300 がネットワークを介して EC サーバ 100 をアクセスしてもよい。

【0018】

続いて本発明にかかる半導体メモリカードの生産行為の形態について説明する。本発明に係る半導体メモリカードは、図 2、図 3 の内部構成に基づいて工業的に生産することができる。

図 2 に示すように、本発明にかかる半導体メモリカードの内部には、コネクタ、耐タンパ性を有する耐タンパモジュールチップ (Tamper Resist Module (TRM)) 1、256M バイトもの容量をもつ EEPROM チップ (図中の EEPROM) 2 が実装されている。

【0019】

耐タンパ性には、諸説があるが、概して以下のことを意味するとされている。

- ①チップを物理的に開梱しても、内部構成は判読不可能である。
- ②電磁波を照射しても内部構成は判読不可能である。
- ③入力データのデータ長と、処理時間との関係がノンリニアである。
- ④入力データによりエラーが発生した際の処理結果により、出力データが逆算されない。

【0020】

これら①～④の性質をもつため、TRM 1 は多くのリバース行為に耐性をもつ。以降、TRM 1 内のハードウェア要素について説明する。

図 3 は、TRM 1 内のハードウェア構成を示す図である。図 3 に示すように TRM 1

には、内部EEPROM 3、外部メモリ制御部 4、HIM 5、マスクROM 6、CPU 7が実装されており、マイコンシステムを形成している。

【0021】

内部EEPROM 3は、読み出し／書き込みが可能なメモリである。TRM 1として実装されたマイコンシステムは、単位面積当たりの製造コストが高く、TRM 1内の内部EEPROM 3の規模は、32Kバイトになっている。この内部EEPROM 3と区別するため、図2に示したEEPROMを、以降外部EEPROM 2と呼ぶ。

外部メモリ制御部 4は、外部EEPROM 2のアクセスのために設けられた専用回路である。外部EEPROM 2のアクセスは、SDポータブルデバイス 300が発するSDコマンドに基づき行われる。

【0022】

HIM(Host Interface Module) 5は、SDポータブルデバイス 300から発行されるSDコマンドのコマンド番号を参照し、そのコマンド番号によりSDコマンドの振り分けを行う。SDコマンドの番号には、1～mの数値と、m+1以上の拡張番号とがある。番号が1～mなら外部メモリ制御部 4にSDコマンドを出力し、m+1以上ならSDコマンドにカプセル化されたECコマンドを取り出して、CPU 7側へと出力する。

【0023】

マスクROM 6は、OS(Operation System)、Java(登録商標)仮想マシン、アプリケーションプログラムが予め格納されている読出専用メモリである。SDポータブルデバイス 300は、このマスクROM 6の固定番地からブートストラップを行うことにより、ECモードとして起動する。

CPU 7は、マスクROM 6に格納されているプログラムを実行する。

【0024】

図4は、図3のTRM 1内のマスクROM 6とCPU 7とからなる部分を、ソフトウェア構成に置き換えて描いた図である。破線枠wk1内は、非接触ICカードと互換性があるモジュールである。一方TRM 1において破線枠外の部分は、SDメモリカードと互換性があるモジュールである。

SDメモリカードとの互換部分は、外部メモリ制御部 4と、HIM 5とからなる。この中でHIM 5は、SDメモリカードにおける機能を踏襲しつつも、非接触ICカー

ド互換モジュールとの窓口としての機能を果たす。

【0025】

非接触ICカード互換モジュールは、レイア構造をもつ。このレイア構造では、最下位層(物理層)に内部EEPROM 3があり、この内部EEPROM 3の上位層にOS 10が、更に上位層にはJava(登録商標)仮想マシン 9が、最上位層にはECクライアントアプリ 8がある。SDメモリカードとの互換部分である外部メモリ制御部 4は、内部EEPROM 3と同じく物理層にあることは注意されたい。

【0026】

以降、図4に示したソフトウェア構成(ECクライアントアプリ 8、Java(登録商標)仮想マシン 9、OS 10)について説明する。

クライアントアプリ 8は、ECクライアントアプリ 8はJava(登録商標)言語で記述されたECアプリの一種であり、ユーザの操作に基づきECサーバ 100にアクセスする。ECサーバ 100におけるサーバアプリは、ECサービス毎の複数種類のものが存在するので、SDeXメモリカードにおけるクライアントアプリも、ECサービス毎の複数種類のものが存在する。図中のC_APL1,2,3...nは、ECサーバ 100におけるサーバアプリS_APL1,2,3...nのそれぞれについて、クライアントアプリが存在することを示す。クライアントアプリ 8がカードリーダーライタ 200、無線基地局 210やネットワークを介して、ECサーバ 100上のECアプリとコマンドの送受信を行うことにより、ECにおける様々なECサービスを享受する。ECアプリから受信したECコマンドがデータの書き込みコマンドである場合、クライアントアプリは、そのECコマンドをJava(登録商標)仮想マシンを介してOS 10に出力する。

【0027】

クライアントアプリ本来の役割の他に、ECクライアントアプリ 8は、ユーザ操作に基づく外部EEPROM 2及び内部EEPROM 3のアクセスをECモードにおいて実行する。このアクセスにはファイルをクリエイトしたり、そのファイルを読み書きしたりするというファイルアクセスが含まれる。

Java(登録商標)仮想マシン 9(図中のJava(登録商標)Card VM)は、Java(登録商標)言語で記述されたECクライアントアプリ 8を、CPU 7のネイティブコー

ドに変換して、CPU 7 に実行させる。

【0028】

OS 10 は、クライアントアプリが発行したコマンドに基づく外部EEPROM 2 及び内部EEPROM 3 の読み書きを実行する。以上が、SDeXメモリカードのソフトウェア構成である。

続いて外部EEPROM 2 及び内部EEPROM 3 における論理フォーマットについて説明する。図 5 は、外部EEPROM 2 及び内部EEPROM 3 の論理フォーマットを示す図である。外部EEPROM 2 及び内部EEPROM 3 は、2つのメモリ空間sm1, sm2を構成している。メモリ空間sm1は、TRM 1 内のCPU 7 からアクセス可能なメモリ空間であり、ECアプリの使用領域 2 1、セキュア領域 2 2 からなる。メモリ空間sm2は、TRM 1 内CPU 7 を介することなく、SDポータブルデバイス 3 0 0 がアクセスすることができメモリ空間であり、認証領域 2 3 と、非認証領域 2 4 とがある。認証領域 2 3、非認証領域 2 4 とは、SDメモリカードがもつメモリ領域であり、その意味合いについては上述した特許文献1(特開2001-14441号公報)を参照されたい。

【0029】

図 6 は、セキュア領域 2 2、認証領域 2 3、非認証領域 2 4 の内部を示す図である。セキュア領域 2 2、認証領域 2 3、非認証領域 2 4 は、ISO/IEC 9293に準拠したファイルシステム構造を有する。ISO/IEC 9293は、説明の便宜のために選んだファイルシステム構造の一例に過ぎず、UDF(Universal Disk Format)等、他のファイルシステム構造を有していてもよい。

【0030】

セキュア領域 2 2 は、TRM 1 内のECアプリの使用領域の拡張領域であり、内部EEPROM 3 上の領域 2 2 aと、外部EEPROM 2 上の領域 2 2 bとからなる。外部EEPROM 2 上の領域 2 2 bには、ファイルシステム領域であるパーティション1, 2, 3...nが存在する。本発明にいう『ファイルシステム領域』は、このパーティションに対応する。一方マスタブートレコードやパーティションへのアクセステーブル(パーティションテーブル1, 2, 3...n)は、内部EEPROM 3 内の領域 2 2 a上にある。

【0031】

SDモードにおいてSDポータブルデバイス 3 0 0 がアクセスできるのは、TRM 1

外の外部EEPROM 2のみであり、TRM 1内のEEPROM 3はアクセスすることができない。この内部EEPROM 3内にマスタブートレコードやパーティションテーブルが存在するので、SDポータブルデバイス 300はセキュア領域 22内のパーティション 1, 2, 3...nを認識することができない。SDポータブルデバイス 300により認識されるのは、マスタブートレコードやパーティションテーブルが外部EEPROM 2内にある認証領域 23、非認証領域 24に限られる。

【0032】

CPU 7によるセキュア領域 22のアクセスは、CPU 7からのアクセス時、つまりECモードでないとなし得ない。このことから外部EEPROM 2、内部EEPROM 3を跨いで存在するセキュア領域 22のアクセスは、ECモードに限られることがわかる。

セキュア領域 22内のパーティションや、認証領域 23のパーティション、非認証領域 24のパーティションは、共通の内部構成を有する。図 7は、パーティションの共通構成を示す図である。

【0033】

パーティションは、パーティションブートセクタ、『二重化ファイルアロケーションテーブル』、『ルートディレクトリエントリ』、ユーザデータ領域からなる。

『パーティションブートセクタ』は、パーティションに関する情報が記述されたテーブルである。

【0034】

『二重化ファイルアロケーションテーブル(File Allocation Table(FAT))』は、ISO/IEC 9293に準拠した2つのFATからなる。各FATは、各クラスタに対応づけられた複数のFATエントリからなる。各FATエントリは、対応するクラスタが使用中であるか、未使用であるかを示すものであり、対応するクラスタが未使用であれば、そのファイルエントリには、“0”が設定され、対応するクラスタが使用中であれば、クラスタ番号が設定される。このクラスタ番号は、対応するクラスタが読み出された場合、次にどのクラスタを読み出せばよいかといったクラスタ間のリンク関係を示す。

【0035】

『ルートディレクトリエントリ』は、ルートディレクトリに存在する複数ファイルについてのファイルエントリを複数含む。各ファイルエントリは、存在するファイルの「ファイル名」と、そのファイルの「ファイル拡張子」と、ファイルの先頭部が格納されている「ファイル最初のクラスタ番号」と、そのファイルについての「ファイル属性」と、ファイルが記録された「記録時刻」と、ファイルの「記録日付」と、ファイルのデータ長である「ファイル長」とを含む。

【0036】

『ユーザ領域』は、ファイルが格納される領域である。以上がパーティションの構成である。続いてパーティションテーブル及びパーティションブートセクタについて説明する。

セキュア領域22のパーティションテーブルは、内部EEPROM3に存在する。一方認証領域23、非認証領域24についてのパーティションテーブルは、外部EEPROM2に存在する点に違いがある。しかし、セキュア領域22、認証領域23、非認証領域24のパーティションテーブルは何れも図8(a)の内部を有する。図8(a)は、パーティションテーブルを示す図であり、図8(b)は、図7のパーティション内のパーティションブートセクタを示す図である。

【0037】

『パーティションテーブル』は、図8(a)の矢印ky2に示すように、“Boot Indicator”と、パーティションの開始ヘッダを特定する“Starting Head”と、パーティションの開始セクタ・開始シリンダを特定する“Starting Sector/Starting Cylinder”と、ファイルシステムのタイプを示す“SystemID”と、“Ending Head”と、パーティションの終了セクタ・終了シリンダを特定する“Ending Sector/Ending Cylinder”と、このパーティションの開始セクタまでの相対セクタ数を示す“Relative Sector”と、パーティションのセクタ数が設定される“Total Sector”とからなる。

【0038】

パーティションブートセクタは、図8(b)に示すような情報項目を有するExtend FDC記述子が設定される。図8(b)によれば、Extend FDC記述子は、Jump Command, Creating System Identifier, 一セクタのサイズ(Sector Size), 一ク

ラスト当たりのセクタ数(Sector per Cluster),Reserved Sector Count,二重化FATに含まれるFAT数(Numbr of FATs),ルートディレクトリエントリのデータ長(Numbr of Root-directory Entries),Total Sectors,Medium Identifier,FAT1つ当たりのセクタ数(Sector Per FAT),Sector Per Track,Number of Sides,Number of Hidden Sectors,総セクタ数(Total Sectors),Physical Disk Number,Extended Boot Record Signature,Volume ID Number,ボリュームラベル(Volume Label),File System Type,Signature Word等の項目が設定される。

【0039】

以上が、TRM1の内部構成である。続いて、領域拡張部11について説明する。以下、この領域拡張部11を設けたことの技術的意義を説明する。

非接触ICカード互換モジュールにおいて、ECアプリから受信したデータは、内部EEPROM3に書き込まれる。ECアプリから書き込みが要求されるデータは、金銭に係るものであり、大半がサイズが小さく内部EEPROM3でも充分収まる。ところが年間の取引引き明細に関するデータ書き込みがECアプリから要求された場合、サイズが余りにも大きく内部EEPROM3の容量では不足が生ずる。だからといってかかるデータを外部EEPROM2にそのまま書き込むのは、セキュリティ上好ましくない。何故なら、かかる年間の取引明細は、金銭に至らないまでも、それに準ずる保護価値があるからである。

【0040】

そこで領域拡張部11は、TRM1に準ずるセキュリティを保証しつつ、ECアプリの使用領域を、内部EEPROM3から外部EEPROM2へと拡張する。

領域拡張部11は、ECアプリのECアプリの使用領域の拡張にあたって、ECアプリに外部EEPROM2内の1つのファイルシステムを割り当てる。ECアプリに割り当てられたファイルシステムは、そのECアプリ固有のものであり、他のECアプリはこのファイルシステムをアクセスすることはできない。1つのファイルシステム内部という閉じた空間にて、ECアプリは自由にファイルアクセスを行うことができる。領域拡張部11により割り当てられるファイルシステムとは、上述したセキュア領域内のパーティションである。領域拡張部11によるアタッチは、クライアントアプリがファイルシステムOPENを要求した際になされる。ファイルシ

テムOPENが要求された際、領域拡張部11は外部EEPROM2内に1つのパーティションを生成し、そのパーティションについてのパーティションテーブルを配置する。そしてECアプリには、ファイルシステムを利用するためのAPL-IDを付与する。このAPL-IDは、10桁以上のランダムな数値からなり、パスワードのように用いられる。

【0041】

領域拡張部11から付与されたこのAPL-IDを利用することで、ECアプリは自身に割り当てられたファイルシステムにデータを書き込んだり、データを読み出したりすることができる。ファイルシステムのOPENは、いわゆるファイルオープンとは異なる。従ってECアプリがセキュア領域22のファイルをオープンするには、前もってファイルシステムをOPENし、その後、ファイルをOPENするという二段階のOPENを行わねばならない。

【0042】

ECアプリによるデータ読み書きが終われば、ファイルシステムのデタッチを行う。ファイルシステムのデタッチとは、ECアプリに割り当てられたパーティションを解放することである。領域拡張部11によるデタッチは、クライアントアプリがファイルシステムCLOSEを要求した際になされる。ファイルシステムCLOSEが要求された際、デタッチは、領域拡張部11によりなされる。ファイルシステムのCLOSEも、いわゆるファイルCLOSEとは異なる。ECアプリがセキュア領域22のファイルをCLOSEした後に、その後、ファイルが存在するファイルシステムをCLOSEするという二段階のCLOSEを行わねばならない。以降、同じECアプリが、同じパーティションを利用するには、APL-IDにより自己の正当性を証明した上で、領域拡張部11にアタッチを行わせねばならない。

【0043】

図9は、ECサーバ100によるSDeXメモリカードのアクセス、SDポータブルデバイス300によるSDeXメモリカードのアクセスを示す図である。図中の実線の矢印jt1,jt2,jt3は、ECサーバ100によるSDeXメモリカードのアクセスを模式的に示す。図中の破線の矢印hs1は、SDポータブルデバイス300によるSDeXメモリカードのアクセスを模式的に示す。本図に示すように、ECアクセスは、内部

EEPROM 3、外部EEPROM 2内のセキュア領域 22の何れかにアクセス可能であり、ECサーバ 100内のECアプリは、書き込むべきデータの大きさや重要度に応じて、書込先を選ぶことができる。

【0044】

図10は、SDeXメモリカード、SDポータブルデバイス 300、ECサーバ 100間におけるコマンド・レスポンスのシーケンス図である。本図において右向きの矢印はコマンドを示し、左向きの矢印は、レスポンスを示す。

SDモードでは、SDポータブルデバイス 300がホスト装置であり、SDポータブルデバイス 300はHIM5を介してSDeXメモリカードの外部メモリ制御部4と、SDコマンド、SDレスポンスの送受信sc1,2,3,4を行う。

【0045】

ECモードにおけるシーケンスは、このSDモードにおけるシーケンスを踏襲しつつも、これを応用したものになっている。ECモードにおいても、SDモード同様HIM5を介した外部メモリ制御部4とのコマンド・レスポンスの送受信sc5,6が行われる。これらのコマンド・レスポンスは、ECコマンドをカプセル化したSDコマンド、ECレスポンスをカプセル化したSDレスポンスであり、SDポータブルデバイス 300は、HIM5を介したコマンド・レスポンスの送受信に加え、カードリーダー 200、無線基地局 210、ネットワークを介したECサーバ 100とのECコマンド、ECレスポンスの送受信sc7,8を行う。ECコマンド、ECレスポンスの送受信sc5,6を行う点が、第1の差違点である。ECサーバ 100との送受信において、SDポータブルデバイス 300はその内部で、ECコマンド・ECレスポンスと、SDコマンド、SDレスポンスとの相互変換を行う。

【0046】

SDモードとの第2の差違は、SDモードにおいてコマンド・レスポンスは外部メモリ制御部4-HIM5をダイレクトに行き来する。これに対し、ECモードではコマンド・レスポンスが非接触ICカード互換モジュールのクライアントアプリ8、領域拡張部11を経由する点、つまりクライアントアプリ8、領域拡張部11を通る。この迂回部分uc1,2,3,4,5,6,7が存在する点が第2の差違点である。

【0047】

迂回部分において、外部EEPROM 2 への書き込みに先立ち、クライアントアプリは、ファイルシステムのOPEN、ファイルOPENを順次行う。ファイルシステムのOPENが命じられれば領域拡張部 11 は、ファイルシステムのアタッチを行う。

一方外部EEPROM 2 の書き込み後、クライアントアプリは、ファイルのCLOSE、ファイルシステムのCLOSEを行う。ファイルのCLOSEが命じられれば領域拡張部 11 は、ファイルシステムのデタッチを行う。

【0048】

以上のように本実施形態によれば、TRM 1 の内部EEPROM 3 から外部EEPROM 2 へとECアプリの使用領域を拡張するにあたって、ECアプリの使用領域の拡張部にあたるパーティションを外部EEPROM 2 内に配置しつつも、パーティションテーブルをTRM 1 内部に置く。拡張部の根幹であるパーティションテーブルをTRM 1 内に秘匿するので、ECアプリの使用領域の拡張部がどこから始まるかを悪意をもったものに知られずに済む。これにより、ECアプリにより書き込まれたデータの守秘性を保つことができる。

【0049】

また、ECアプリのそれぞれにパーティションを割り当て、各パーティションの関係を排他的なものにするので、複数ECアプリのうち1つが、悪意をもったものが操作されたとしても、他のECアプリに割り当てられたパーティションの格納内容が、そのECアプリに知られることはない。1つのECアプリによる不正アクセスを、他のECアプリに波及させないので、格納内容の守秘性を保つことができる。

【0050】

(第2実施形態)

第2実施形態は、第1実施形態より強固に、セキュア領域 22 の格納内容を保護する改良に関する。SDeXメモリカードの格納内容の保護は、一般に格納内容を暗号化することで実現される。

しかし不正なECアプリによりセキュア領域 22 がアクセスされる場合、セキュア領域 22 の格納内容を暗号化する暗号鍵が、そのECアプリを操作する者により暴露される恐れがある。そうした場合、セキュア領域 22 をアクセスする他のECアプリの格納内容までも、暴露される恐れがあり、セキュア領域 22 をアクセス

する他のECアプリのECプロバイダに損害が波及する。

【0051】

セキュア領域22の格納内容の全暴露を避けるべく、本実施形態ではパーティションを各ECアプリに割り当てる際、OS10は固有の暗号鍵をECアプリに割り当てる。そして各ECアプリが、自身のセキュア領域上のファイルシステムをアクセスする際、ファイルシステムに書き込まれるべきデータ、ファイルシステムから読み出されるべきデータを固有の暗号鍵で暗号化・復号化する。各ECアプリにパーティションを割り当てることに加え、固有の暗号鍵で暗号化・復号化を行うので、たとえ1つのECアプリを操作するユーザが自身に割り当てられた暗号鍵をつきとめたとしても、他のECアプリに対応する暗号鍵が暴露されることはない。

【0052】

以上の暗号化・復号化を行うため、OS10は、図11に示す構成をもつ。図11に示すようにOS10は、第1実施形態に示した領域拡張部11に加え、選択テーブル12、暗号化テーブル13、暗復号化部14を有する。

選択テーブル12は、複数のビット長と、複数の暗号方式とを対応付けたテーブルである。ビット長は、ECアプリに固有の暗号鍵を生成する際、暗号鍵をどれだけのビット長にするかを示す。暗号方式は、その暗号鍵をもって、どのような暗号化アルゴリズムで暗号化するかを示す。これら複数の暗号方式、ビット長は、1～Lのレベル値があり、高いレベル値には、難易度が高いアルゴリズムの暗号方式と、長いビット長とが対応づけられている。低いレベル値には、難易度が低いアルゴリズムの暗号方式と、短いビット長とが対応づけられている。暗号方式の難易度が高い程、暗号鍵のビット長が長い程、パーティションの格納内容のセキュリティは高くなることを意味する。セキュリティレベルの高低は、暗号化の処理時間と比例関係になる。つまり暗号方式の難易度が高い程、暗号鍵のビット長が長い程、暗号化、復号化に費やされる時間は長くなる。逆に暗号方式の難易度が低い程、暗号鍵のビット長が短い程、パーティションの格納内容のセキュリティは甘くなり、暗号化、復号化に費やされる時間は短くなる。

【0053】

暗号化テーブル13は、APL-ID、暗号方式、ビット長の対応をとるテーブルで

ある。

暗復号化部 14 は、領域拡張部 11 がパーティションを EC アプリに割り当てる際、EC クライアント アプリ 8 からセキュリティレベルを受け取って、選択テーブル 12 からそのセキュリティレベルに対応する暗号方式と、ビット長とを選択テーブル 12 から検索して(図中の rf1, rf2)、検索したビット長の乱数を発生する。そうして発生した乱数を暗号鍵として固有の暗号鍵を EC アプリに割り当てる。この割り当て結果は、暗号化テーブル 13 に示される(図中のレコード追加)。以降この EC アプリがデータを書き込む際、その EC アプリから受け取ったデータを(図中の Write data)、割り当てられた暗号鍵を用いてデータを暗号化した上で外部メモリ制御部 4 に出力する(図中の暗号化 Write data)。また EC アプリがデータを読み出す際、暗復号化部 14 は外部メモリ制御部 4 から受け取ったデータを(図中の暗号化 Read data) その EC アプリに割り当てられた暗号鍵を用いてデータを復号化した上で、EC クライアント アプリ 8 に引き渡す(Read data)。

【0054】

第 2 実施形態に係る領域拡張部 11 及び暗復号化部 14 は、図 12 (a) ~ (c) のフローチャートの処理を行うプログラムをコンピュータ記述言語で記述して、CPU 7 に実行させることにより生産される。

図 12 (a) は、領域拡張部 11 及び暗復号化部 14 の処理手順を示すフローチャートである。

【0055】

図 12 (a) のフローチャートにおけるステップ S1 ~ ステップ S4 は、領域拡張部 11 の処理手順を示す。ステップ S1 で、領域拡張の要求元の EC アプリに未割当パーティション番号 i をアサインし、ステップ S2 では、i 番目パーティションについてのパーティションテーブルを内部 EEPROM 3 に書き込み、外部 EEPROM 2 にパーティションを生成する。ステップ S3 において、パスワードを生成し、ステップ S4 では、生成したパスワードを APL-ID として要求元アプリに通知する。

【0056】

また、図 12 (a) のフローチャートにおけるステップ S5 ~ ステップ S7 は

、暗復号化部 14 の処理手順を示す。ステップ S 5 では、拡張要求時のセキュリティレベルに応じた暗号方式、ビット長を選択テーブルから取り出す。ステップ S 6 では、取り出されたビット長の乱数を生成し、ステップ S 7 では、取り出された暗号方式、ビット長、生成した乱数からなるレコード i を暗号化テーブルに追加する。

【0057】

図 12 (b) は、領域拡張部 11 及び暗復号化部 14 によるファイル書き込みの処理手順を示すフローチャートである。

ステップ S 11 において、領域拡張部 11 は書込を行うアプリに割り当てられた APL-ID を取得し、ステップ S 12 では、APL-ID からパーティション番号 i を特定し、アプリから、パラメータ buf, file, fp の設定を受け付ける。

【0058】

ここで受け付けられるパラメータには、以下のものがある。

buf:書き込むべきデータへのポインタ

file:書込先ファイルのファイル名

fp:書込先ファイル内部におけるポインタ

ステップ S 13 において暗復号化部 14、buf 内のデータを、レコードにおける暗号鍵 i を用いて暗号方式 i で暗号化し、ステップ S 14 において領域拡張部 11 はパーティション i のファイルにおいてファイルポインタ以降に、暗号化データを書き込む。

【0059】

図 12 (c) は、領域拡張部 11 及び暗復号化部 14 によるファイル読み出しの処理手順を示すフローチャートである。ステップ S 21 において領域拡張部 11 は、読出を行うアプリに割り当てられた APL-ID を取得し、ステップ S 22 において領域拡張部 11 は、APL-ID からパーティション番号 i を特定する。そしてステップ S 23 において領域拡張部 11 は、アプリから、パラメータ buf, file, fp, size の設定を受け付ける。

【0060】

このステップ S 23 で受け付けられるパラメータには、以下のものがある。

buf:読み出すべきデータへのポインタ

file:読出先ファイルのファイル名

fp:読出先ファイル内部におけるポインタ

size:読出データ長

ステップS 24において領域拡張部11はパーティションiのファイルにおいてファイルポインタ以降の暗号化データをsizeだけ読み出し、ステップS 25において暗復号化部14は、暗号鍵iを用いて読み出されたデータを、暗号方式iで復号化して、バッファに格納する。

【0061】

以上のように本実施形態によれば、ECアプリは、セキュリティレベルと処理時間との関係を考慮して、セキュリティレベルを引数に指定してアタッチをOS10に要求することができる。これにより、自身がどれだけのセキュリティレベルを要求しているかをOS10に伝えることができる。

尚、セキュリティレベルはECアプリから受け付けるとしたが、OS10側で自動的に設定するものとしてもよい。また、選択テーブル12における暗号方式やビット長は、バージョンアップできるようにしてもよい。これにより、セキュア領域の守秘性を高めることができる。

【0062】

(第3実施形態)

第2実施形態では、ECアプリがセキュア領域22の使用を要求する毎に、そのECアプリに新たにパーティションをアタッチした。そうすると、セキュア領域22の使用を要求するECアプリが増えれば、TRM1内は多くのパーティションについてのパーティションテーブルを格納せねばならず、内部EEPROM3に不足がでる。パーティションが多くなった場合、第3実施形態では、一部のパーティションについてのパーティションテーブルを外部EEPROM2内に配置する。この際、パーティションテーブルから、ECアプリに対応するパーティションが判明する恐れがあるので、暗復号化部14はこの外部EEPROM2に置かれたパーティションテーブルは暗号化する。この際、暗復号化部14は外部EEPROM2の他のパーティションに割り当てられたものとは異なった暗号鍵を割り当てる。

【0063】

図13は、本実施形態に係るパーティションテーブルのレイアウトを示す図である。本図に示すように、最後のパーティションテーブルであるパーティションテーブルnは、外部EEPROM2内に置かれている。パーティションテーブルnは、暗号化されており、その暗号鍵は、TRM1の内部EEPROM3のアプリケーション使用領域に配置されている。以降、パーティションnのアクセス時には、このパーティションテーブルnを、この暗号鍵で復号した上でなされる。

【0064】

以上のように本実施形態によれば、他のパーティションとは異なる暗号鍵でアクセステーブルを暗号化して外部EEPROM2に格納するので、内部EEPROM3に不足が生じた場合でも、ある程度のセキュリティレベルをもったパーティションをECアプリに割り当てることができる。

尚、TRM1内のパーティションテーブルであっても外部EEPROM2内にあるパーティションテーブル同様、パーティションとは異なる暗号鍵で暗号化してもよい。

【0065】

(第4実施形態)

Java（登録商標）仮想マシン9上で、複数ECアプリに対応するクライアントアプリが動作している場合、OS10はこれら複数クライアントアプリを、1つのタスクとして認識してしまう。これでは、あるクライアントアプリから他のECアプリへの切り換わり時に、そのECアプリについてのデタッチを行うことができず、その切換先ECアプリが、切換元ECアプリのパーティションをアクセスすることも有り得る。

【0066】

仮に、切換先ECアプリが悪意をもった者に操作されている場合、切換元ECアプリのパーティションの内容がその悪意をもったものに漏洩してしまう恐れがある。本実施形態では、かかる漏洩を避けるため、Java（登録商標）仮想マシン9が、クライアントアプリの切り換えがあれば、その切り換えがあった旨と、切換先APL-IDとを領域拡張部11に通知する。

【0067】

領域拡張部11は、Java（登録商標）仮想マシン9からクライアントアプリの切り換えが通知されれば、ファイルシステムのデタッチを行う。

以上のように本実施形態によれば、Java（登録商標）仮想マシン9を介することにより複数タスクが1つのタスクとして認識される場合であっても、ECアプリの切り換えをJava（登録商標）仮想マシンがOS10に通知するので、クライアントアプリのデタッチを行うことができ、あるクライアントアプリのパーティションの内容を、他のECアプリに漏洩することはない。

【0068】

（第5実施形態）

第3実施形態では、内部EEPROM3の容量が不足した際、パーティションテーブルを外部EEPROM2に配置したが第5実施形態では、内部EEPROM3が不足したかどうかにかかわらずパーティションテーブルを外部EEPROM2に配置する実施形態である。

【0069】

外部EEPROM2に、パーティションテーブルをそのまま配置したのでは外部EEPROM2の何処に各パーティションが存在するのかが明らかである。そこで第5実施形態では、パーティションに対応するパーティションテーブルを暗号化した上で外部EEPROM2に配置しておく。この暗号化にあたっての暗号鍵は、各パーティションテーブル毎に異なるものとし、またパーティションテーブルとのパーティションとの間でも異なるものとする。

【0070】

そしてパーティションテーブルについての暗号鍵は第4実施形態同様、内部EEPROM3に配置しておく。またパーティションのアクセスにあたっては、暗復号化部14にパーティションテーブルの復号を行わせる。

以上のように本実施形態によれば、パーティションテーブルを内部EEPROM3ではなく暗号化した上で外部EEPROM2に配置するので、パーティションの数が多くなっても対処が可能である。

【0071】

(第1実施形態～第5実施形態の補足事項)

(A)尚、ECアプリをアプリケーションプログラムの一例として説明したが、他のECアプリでもよい。鉄道、航空、バス、高速道路等の交通機関が運営するサーバ装置上のサーバアプリケーション、これに対応するクライアントアプリケーションであってもよい。これにより、改札業務や搭乗手続きといった用途でもSDeXメモリカードを利用することができる。

【0072】

また、官公庁や地方公共団体が運営するサーバ装置上のサーバアプリケーション、これに対応するクライアントアプリケーションであってもよい。これにより、住民表や各種証明、登記等の用途にSDeXメモリカードを利用することができる。

(B)図12に示したプログラムによる情報処理は、CPU、EEPROMといったハードウェア資源を用いて具体的に実現されている。つまり、プログラムと、ハードウェアとが協働した具体的手段が、使用目的に応じた情報処理を行うことにより、第1実施形態～第5実施形態に示したSDeXメモリカードは構築される。

【0073】

プログラムによる情報処理が、ハードウェア資源を用いて具体的に実現されていることから、上記フローチャートに処理手順を示したプログラムは、自然法則を利用した技術的思想の創作と捉えることができ、プログラム単体で発明として成立する。図12に示した処理手順は、本発明に係るプログラムの実施行為の形態を開示するものである。

【0074】

尚、第1実施形態～第5実施形態は、SDeXメモリカードに組み込まれた態様で、本発明に係るプログラムの実施行為についての実施形態を示したが、SDeXメモリカードから分離して、第1実施形態～第5実施形態に示したプログラム単体を実施してもよい。プログラム単体の実施行為には、これらのプログラムを生産する行為(1)や、有償・無償によりプログラムを譲渡する行為(2)、貸与する行為(3)、輸入する行為(4)、双方向の電子通信回線を介して公衆に提供する行為(5)、店頭展示、カタログ勧誘、パンフレット配布により、プログラムの譲渡や貸渡を、

一般ユーザに申し出る行為(6)がある。

【0075】

双方向の電子通信回線を介した提供行為(5)の類型には、提供者が、プログラムをユーザに送り、ユーザに使用させる行為や(プログラムダウンロードサービス)、プログラムを提供者の手元に残したまま、そのプログラムの機能のみを電子通信回線を通じて、ユーザに提供する行為(機能提供型ASPサービス)がある。

(C)図12のフローチャートにおいて時系列に実行される各ステップの「時」の要素を、発明を特定するための必須の事項と考える。そうすると、これらのフローチャートによる処理手順は、制御方法の使用形態を開示していることがわかる。これらのフローチャートこそ、本発明に係る制御方法の使用行為についての実施形態である。各ステップの処理を、時系列に行うことで、本発明の本来の目的を達成し、作用及び効果を奏するよう、これらのフローチャートの処理を行うのであれば、本発明に係る半導体メモリカードの制御方法の実施行為に該当することはいうまでもない。

【0076】

(D)第1実施形態～第5実施形態において耐タンパモジュール内外の不揮発メモリをEEPROMとして説明したが、不揮発メモリであればFe-RAM等他のものを採用してもよい。

(E)SDポータブルデバイス300は、携帯電話タイプのものを一例にして説明したが、民生用の携帯オーディオ機器やSTB(Set Top Box)や携帯電話であってもよい。

【0077】

(F)金銭に準ずるセキュアな情報として、年間の取引明細を一例にしたが、機密性が求められる情報であれば、個人情報、企業秘密情報等の他の情報であってもよい。

(G)ECアプリ固有のファイルシステム領域として領域拡張部11は、パーティションを割り当てたが、他の論理領域をECアプリ固有のファイルシステム領域にしてもよい。例えば1つのディレクトリをECアプリ固有のファイルシステム領域にしてもよい。

【0078】

【発明の効果】

以上説明したように本発明に係る半導体メモリカードは、耐タンパモジュールと、不揮発メモリとを備える半導体メモリカードであって、耐タンパモジュールは、内部メモリと、処理部とを含み、耐タンパモジュールの内部メモリには、アプリケーションプログラムにより利用される領域があり、前記処理部は、当該アプリケーションプログラムに固有のファイルシステム領域を不揮発メモリ上に割り当て、当該ファイルシステム領域についてのアクセステーブルを耐タンパモジュールの内部メモリ上に配置することにより、アプリケーションプログラムの利用領域の拡張を行うものである。

【0079】

アクセステーブルを耐タンパモジュールに配置することで、マスタブートレコードーパーティションーディレクトリーファイルというファイルシステムの全体構造がどうなっているかを秘匿することができる。

不揮発メモリのうち、何処から何処までが1つのファイルシステム領域であるか、どこからどこまでが別のファイルシステム領域であるかというファイルシステム領域のアサイン解読が困難であり、ECアプリがどの領域をどのようにアクセスしているかが秘匿される。不揮発メモリにおける第3者によるファイルシステムの全体像の把握が困難であり、不正行為の糸口を与えない。

【0080】

更に、アクセステーブルを耐タンパモジュールの内部メモリに配置することで暗号化を行わなくとも、守秘レベルを保つことができる。そのため、ファイルシステム領域をアクセスするためのオーバーヘッドがなく(つまり、アクセステーブルを暗号化するという保護ではこの暗号化がオーバーヘッドとなり、処理速度の遅延要因になる)、良好な処理速度を保つことができる。

【0081】

ここで前記処理部は、使用領域の拡張にあたって、拡張領域を利用するアプリケーションプログラムに固有の暗号鍵を割り当て(1)、アプリケーションプログラムが前記拡張領域にデータを書き込もうとする際、当該データを暗号化し(2)

、アプリケーションプログラムが当該拡張領域からデータを読み出そうとする際、当該データを復号化する(3)暗復号化部を備えてもよい。

【0082】

ECアプリに固有の暗号鍵を割り当てた上で、ファイルシステム領域の読み書きをECアプリに行わせる。半導体メモリカードが複数ECアプリによりアクセスされ、そのうち1つのECアプリが自身に割り当てられた暗号鍵を暴露したとしても、他のECアプリが半導体メモリカードに書き込んだデータは、その暗号鍵では復号化しえない。1つのECアプリにおける暗号鍵暴露の影響を、他のECアプリに波及させないので、ECアプリが半導体メモリカードに書き込んだデータの守秘性を高めることができる。

【0083】

ここで前記処理部は、アプリケーションプログラムからセキュリティレベルを受け付ける受付部と、セキュリティレベルがとり得る複数の値と、それらの値に対応する暗号鍵のビット長、暗号方式を記憶する記憶部とを備え、前記暗復号化部により割り当てられる暗号鍵は、受付手段が受け付けたセキュリティレベルに対応するビット長に基づき生成され、前記暗復号化部による暗号化及び復号化は、受付手段が受け付けたセキュリティレベルに対応する暗号方式に基づきなされてもよい。

【0084】

ECアプリはデータの読み書きにあたって、データの重要性和、そのデータの読み書きに費やす処理とからセキュリティレベルを設定して、そのセキュリティレベルに基づく、データ読み書きを半導体メモリカードの処理部に求めることができる。そのためデータサイズが大きく、重要度が低いデータは、セキュリティレベルを低く設定してデータ書き込みが短期間に終了するよう、ユーザに配慮することができる。

【0085】

ここで前記処理部は、別のアプリケーションプログラムの利用領域の拡張を、不揮発メモリ上に別のアプリケーションプログラムについてのファイルシステム領域を割り当て、同不揮発メモリ上に当該ファイルシステム領域についてのアク

セステーブルを配置することにより行い、前記暗復号化部は、ファイルシステム領域とは異なる暗号鍵をアクセステーブルに割り当てて、その暗号鍵で、アクセステーブルを暗号化した上で不揮発メモリ上に配置しても良い。耐タンパモジュールにおける内部メモリの容量が小さく、複数ファイルシステム領域のうち何れかのファイルシステム領域テーブルが内部メモリに格納しえない場合でもECアプリに固有のファイルシステム領域を割り当てることが可能になる。

【図面の簡単な説明】

【図 1】 SDeXメモリカードの使用環境を示す図である。

【図 2】 本発明にかかる半導体メモリカードの内部構成を示す図である。

【図 3】 TRM 1 内のハードウェア構成を示す図である。

【図 4】 図 3 のTRM 1 内のマスクROM 6 とCPU 7 とからなる部分を、ソフトウェア構成に置き換えて描いた図である。

【図 5】 外部EEPROM 2 及び内部EEPROM 3 の論理フォーマットを示す図である。

【図 6】 セキュア領域 2 2、認証領域 2 3、非認証領域 2 4 の内部構成を示す図である。

【図 7】 パーティションの共通構成を示す図である。

【図 8】

(a) パーティションテーブルを示す図である。

(b) 図 7 のパーティション内のパーティションブートセクタを示す図である。

【図 9】 ECサーバ 1 0 0 によるSDeXメモリカードのアクセス、SDポータブルデバイス 3 0 0 によるSDeXメモリカードのアクセスを示す図である。

【図 1 0】 SDeXメモリカード、SDポータブルデバイス 3 0 0、ECサーバ 1 0 0 間におけるコマンド・レスポンスのシーケンス図である。

【図 1 1】 第 2 実施形態に係るOS 1 0 の内部構成を示す図である。

【図 1 2】

(a) 領域拡張部 1 1 及び暗復号化部 1 4 の処理手順を示すフローチャートである。

(b) 領域拡張部 11 及び暗復号化部 14 によるファイル書き込みの処理手順を示すフローチャートである。

(c) 領域拡張部 11 及び暗復号化部 14 によるファイル読み出しの処理手順を示すフローチャートである。

【図 13】 第 2 実施形態に係るパーティションテーブルのレイアウトを示す図である。

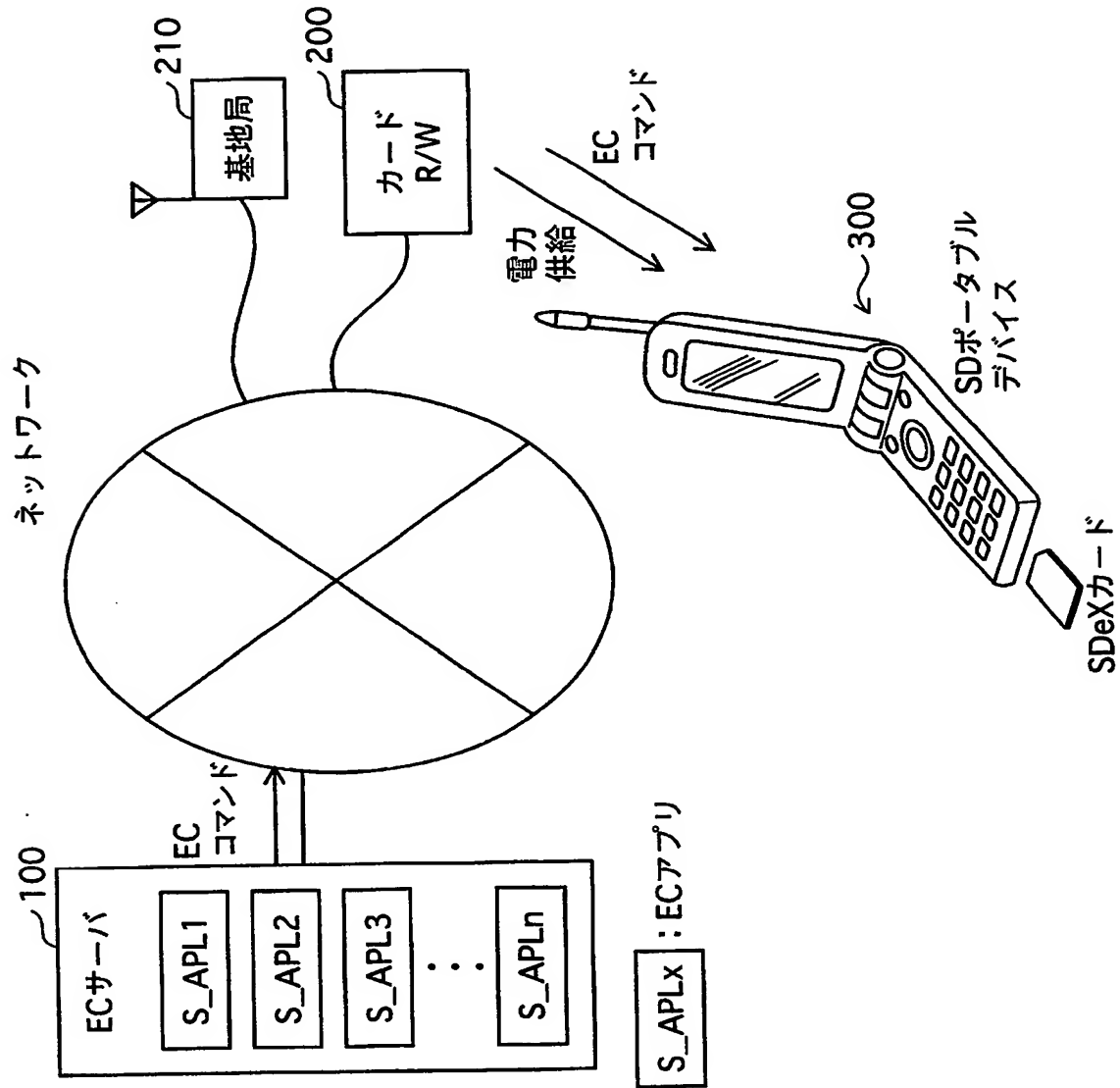
【符号の説明】

- 1 TRM
- 2 外部EEPROM
- 3 内部EEPROM
- 4 外部メモリアクセス部
- 5 HIM
- 6 マスクROM
- 7 CPU
- 8 クライアントアプリ
- 9 仮想マシン
- 10 OS
- 11 領域拡張部
- 12 選択テーブル
- 13 暗号化テーブル
- 14 暗復号化部
- 21 ECアプリの使用領域
- 22 セキュア領域
- 23 認証領域
- 24 非認証領域
- 100 ECサーバ
- 200 カードリーダライタ
- 210 無線基地局
- 300 SDポータブルデバイス

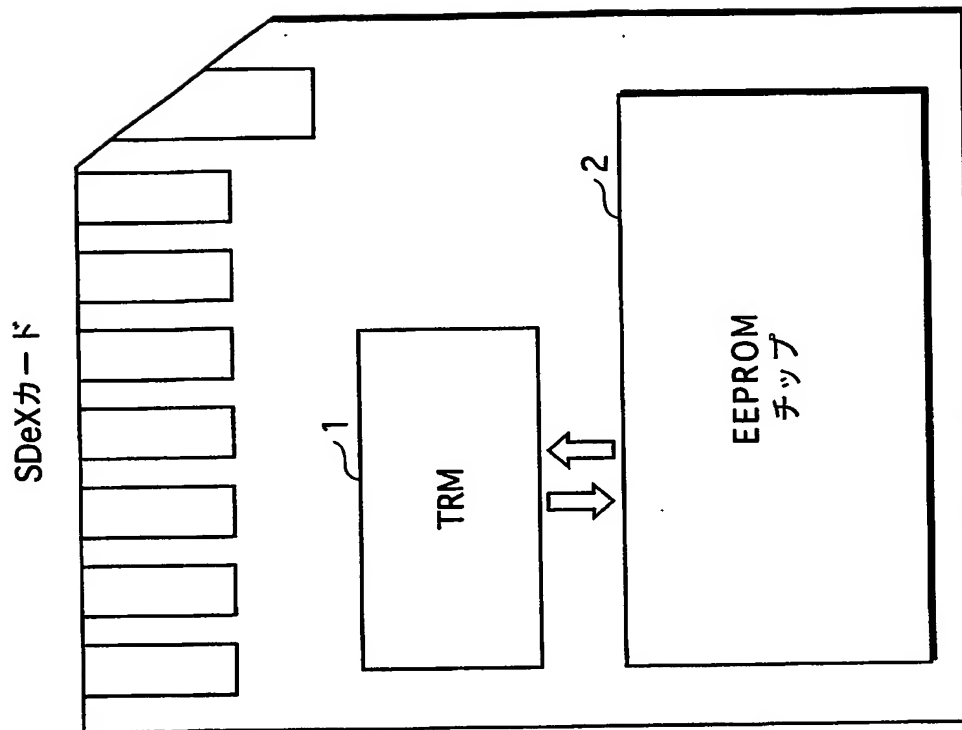
【書類名】

図面

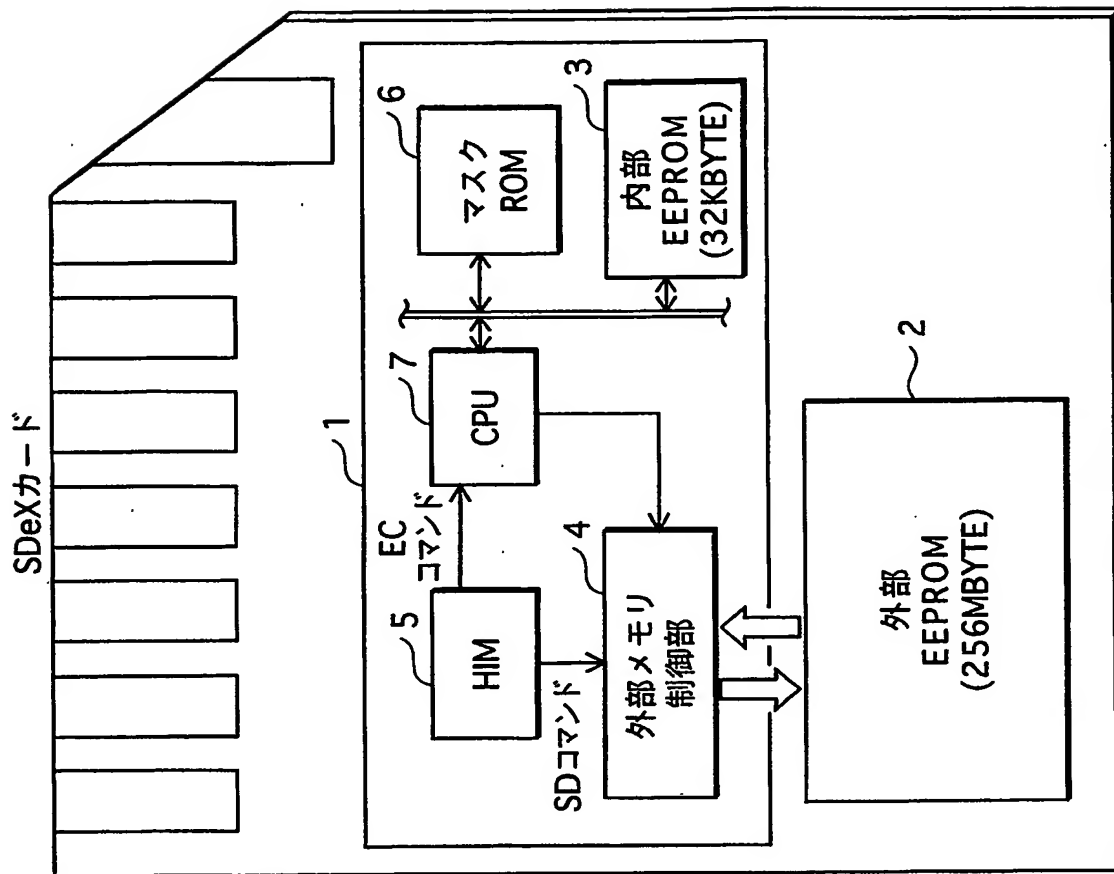
【図1】



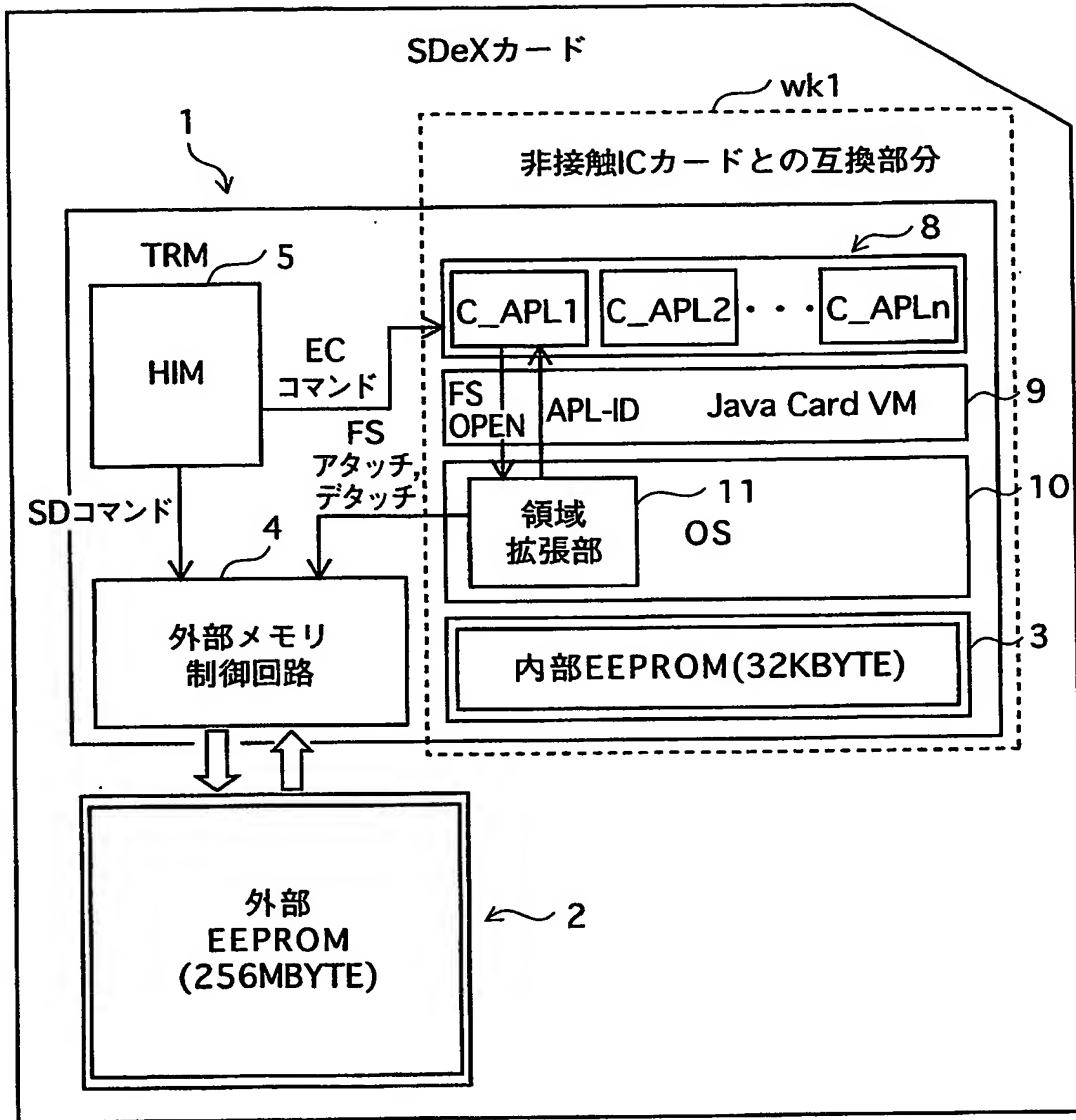
【図 2】



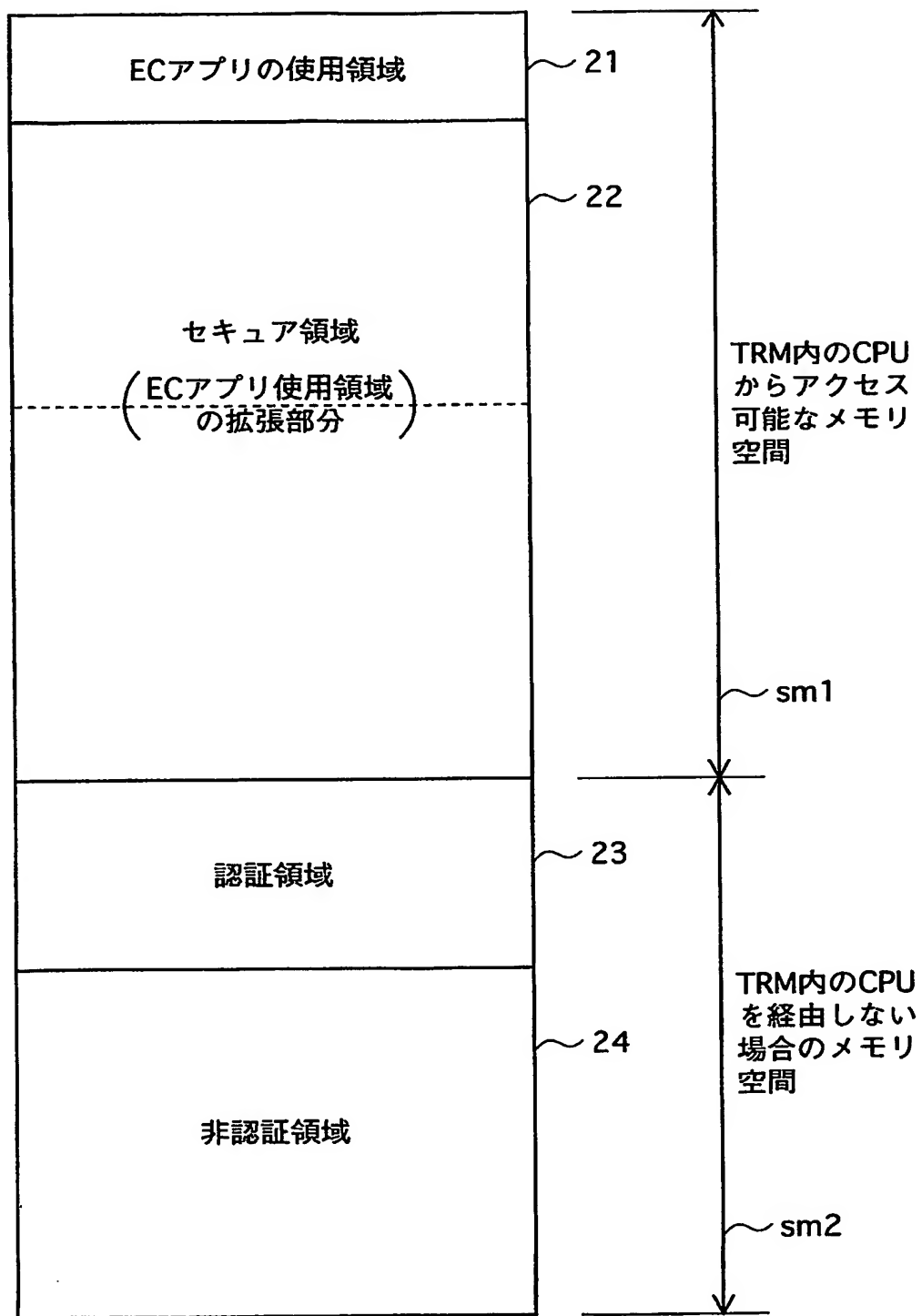
【図 3】



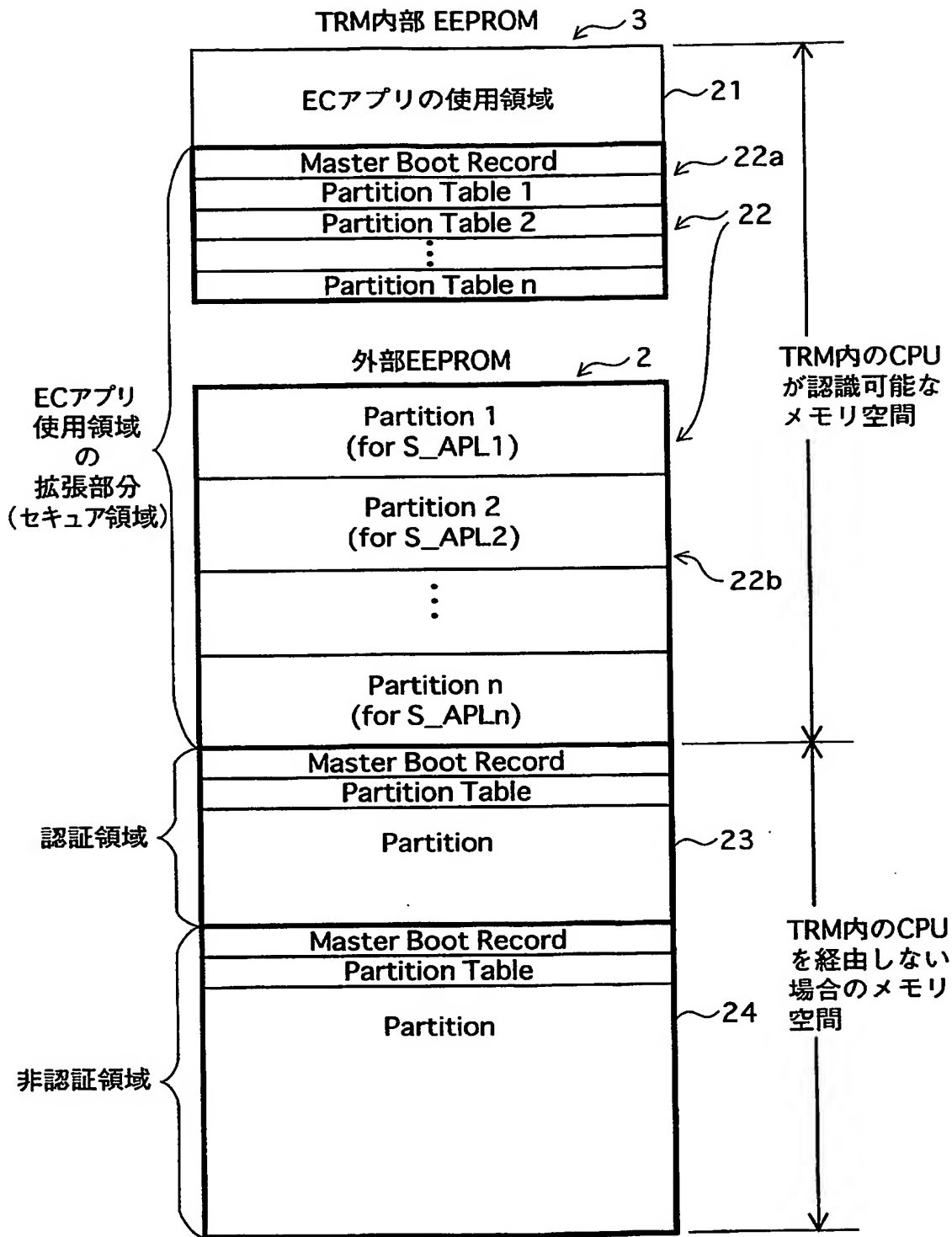
【図 4】



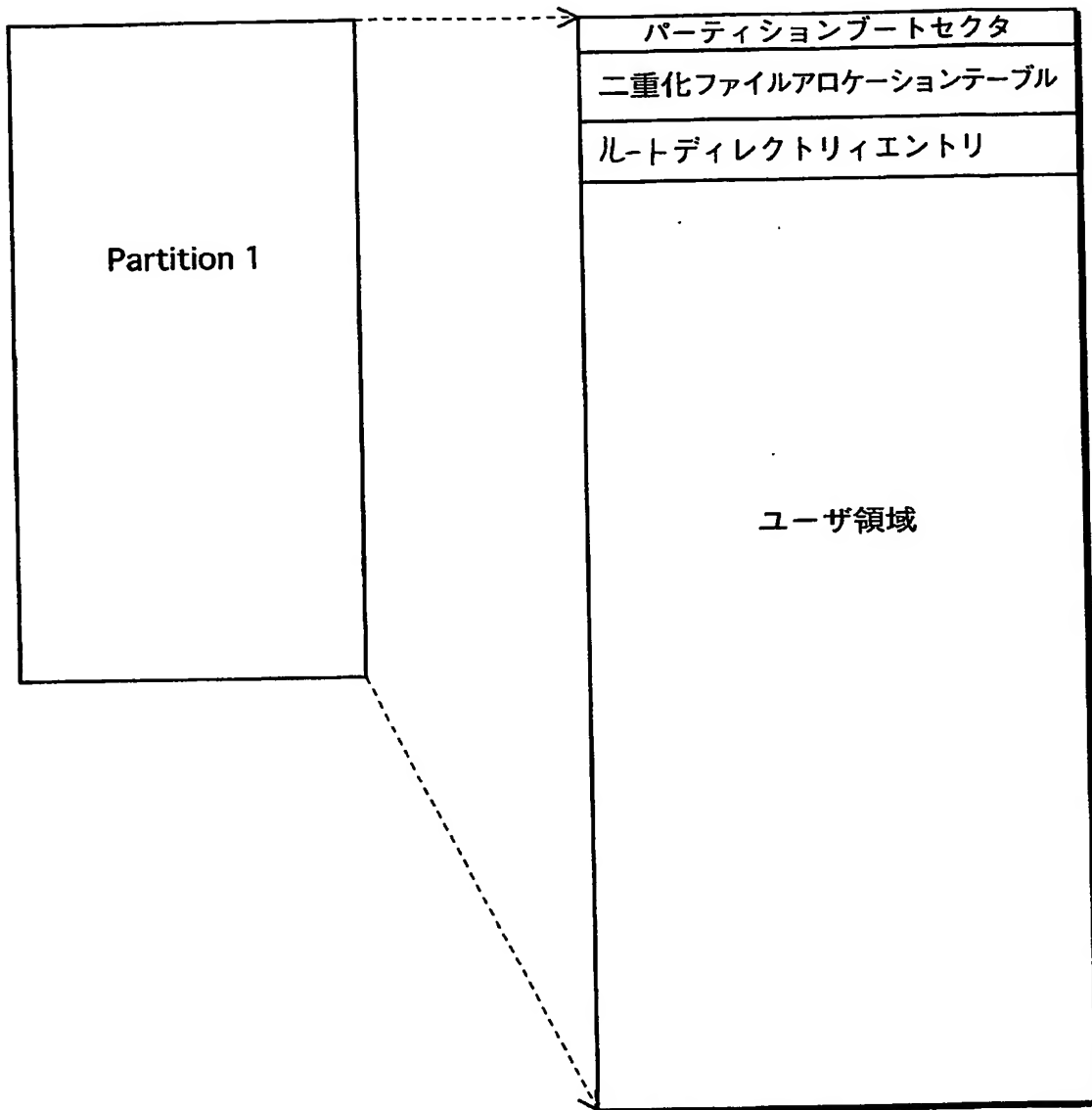
【図 5】



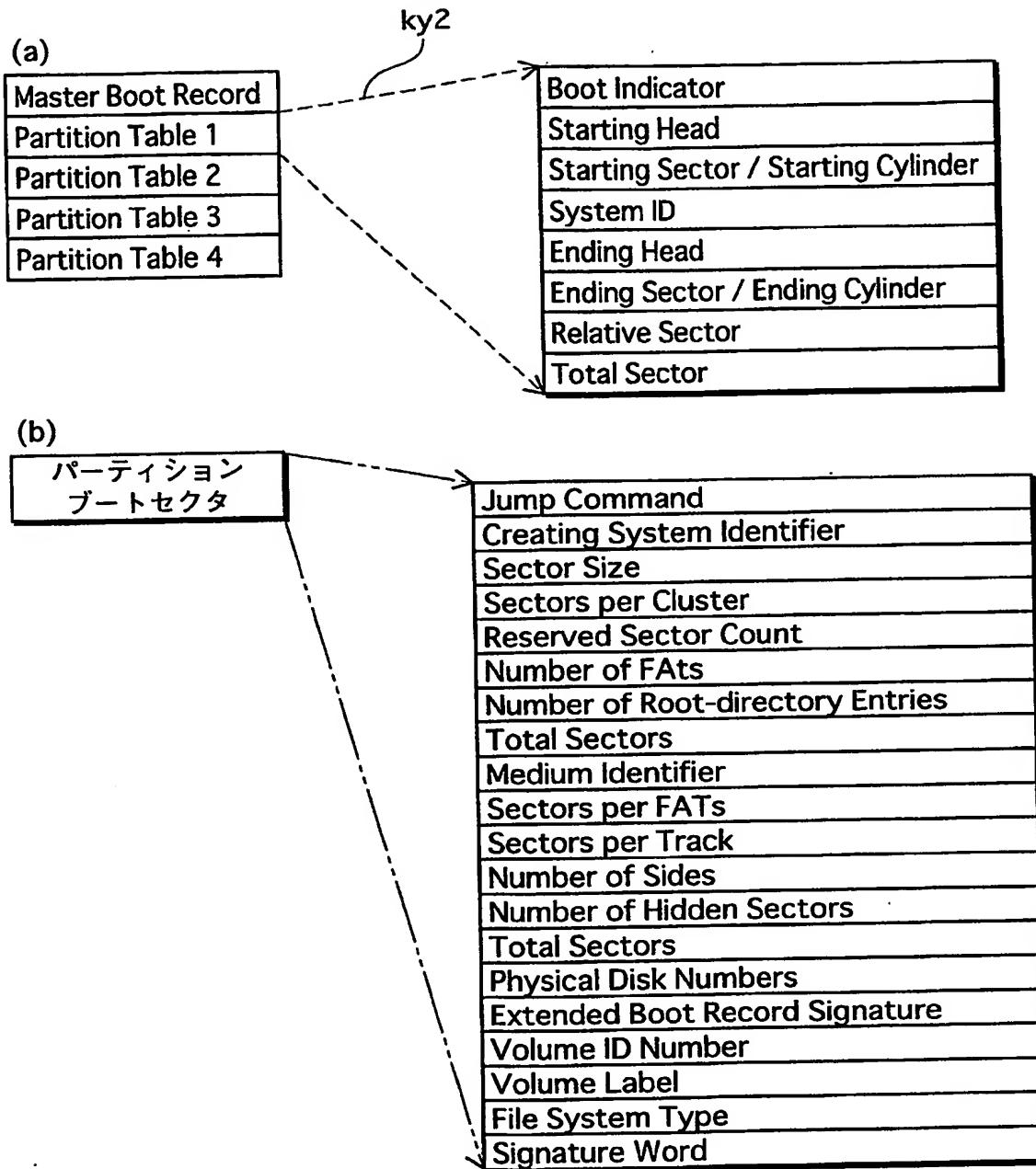
【図 6】



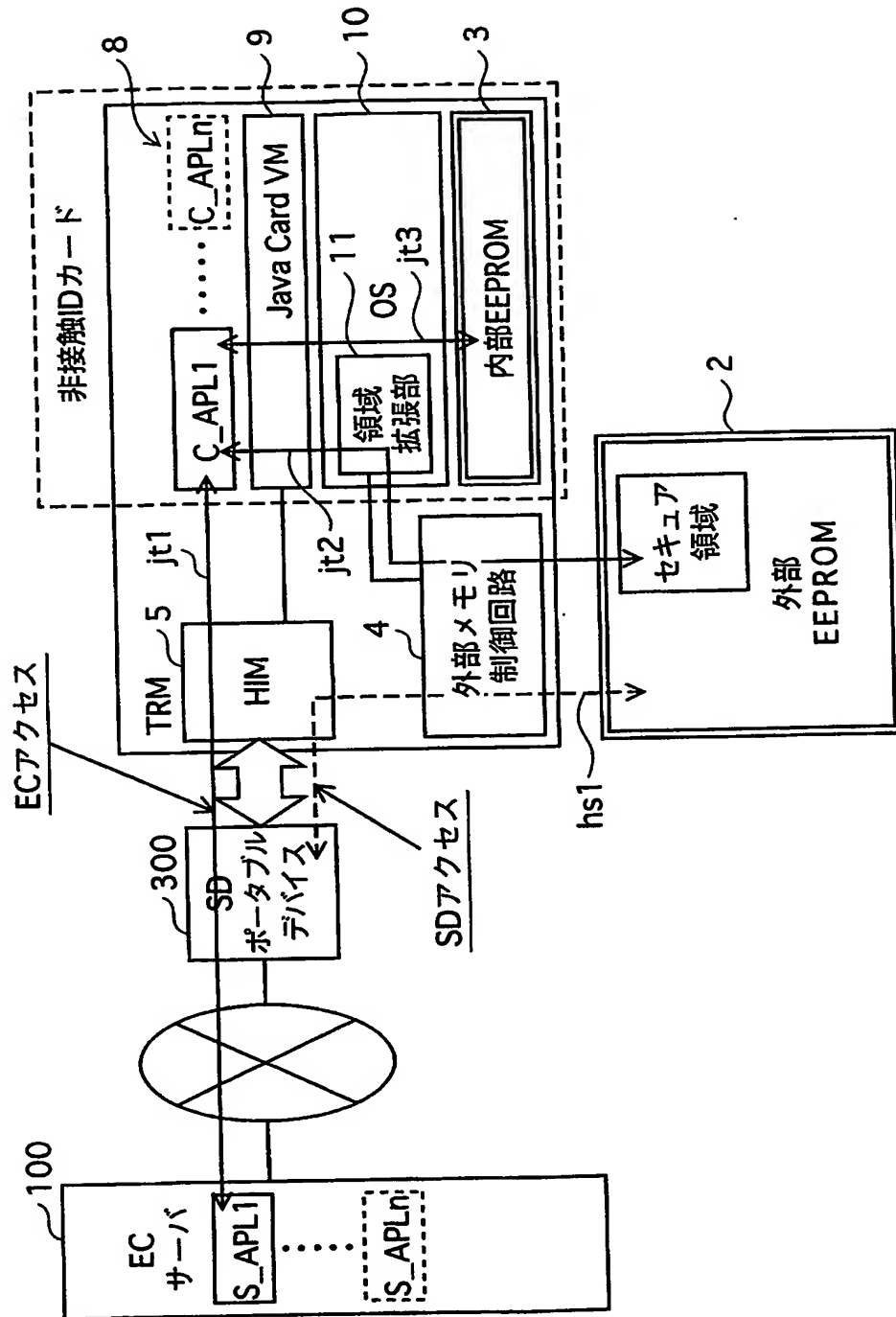
【図 7】



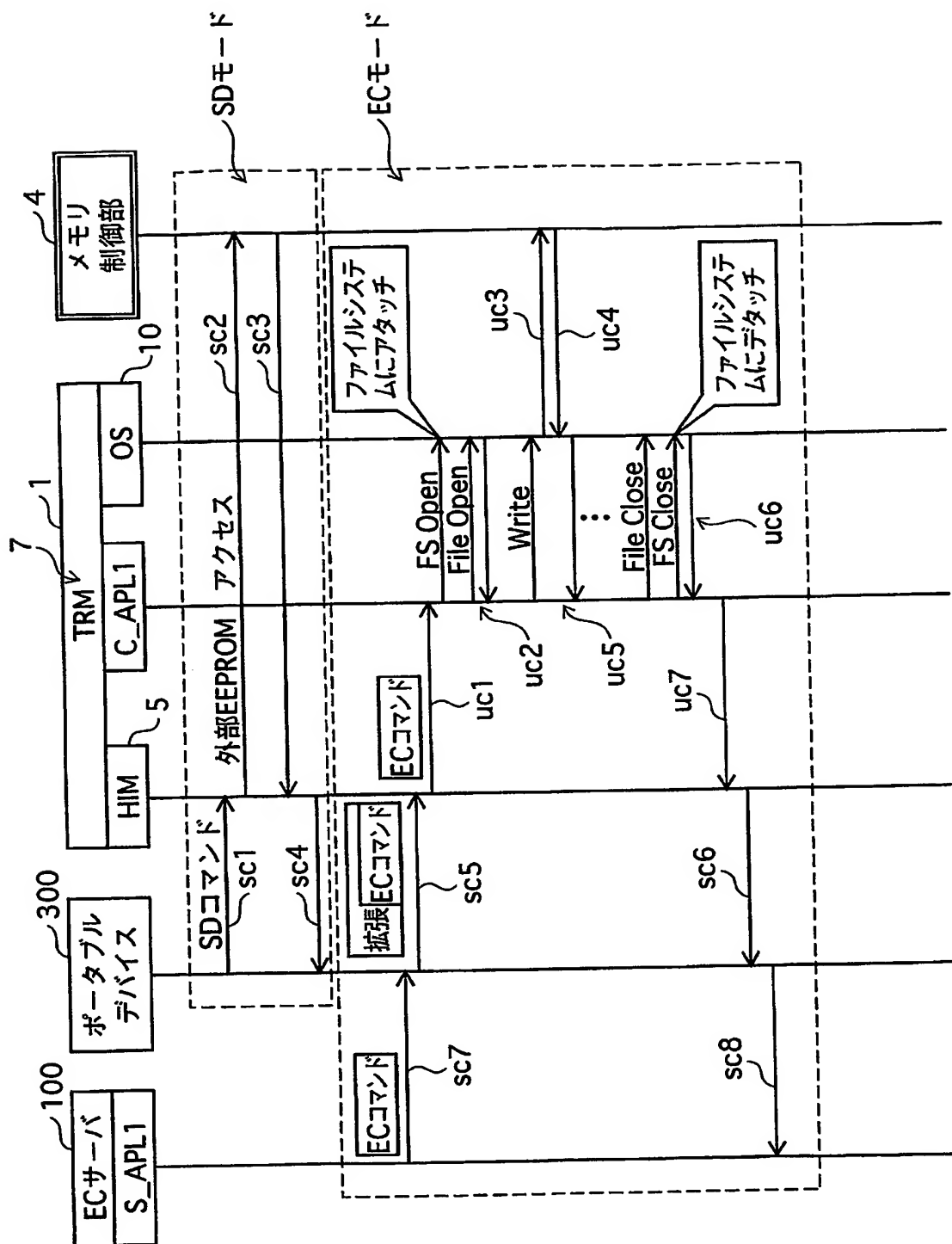
【図 8】



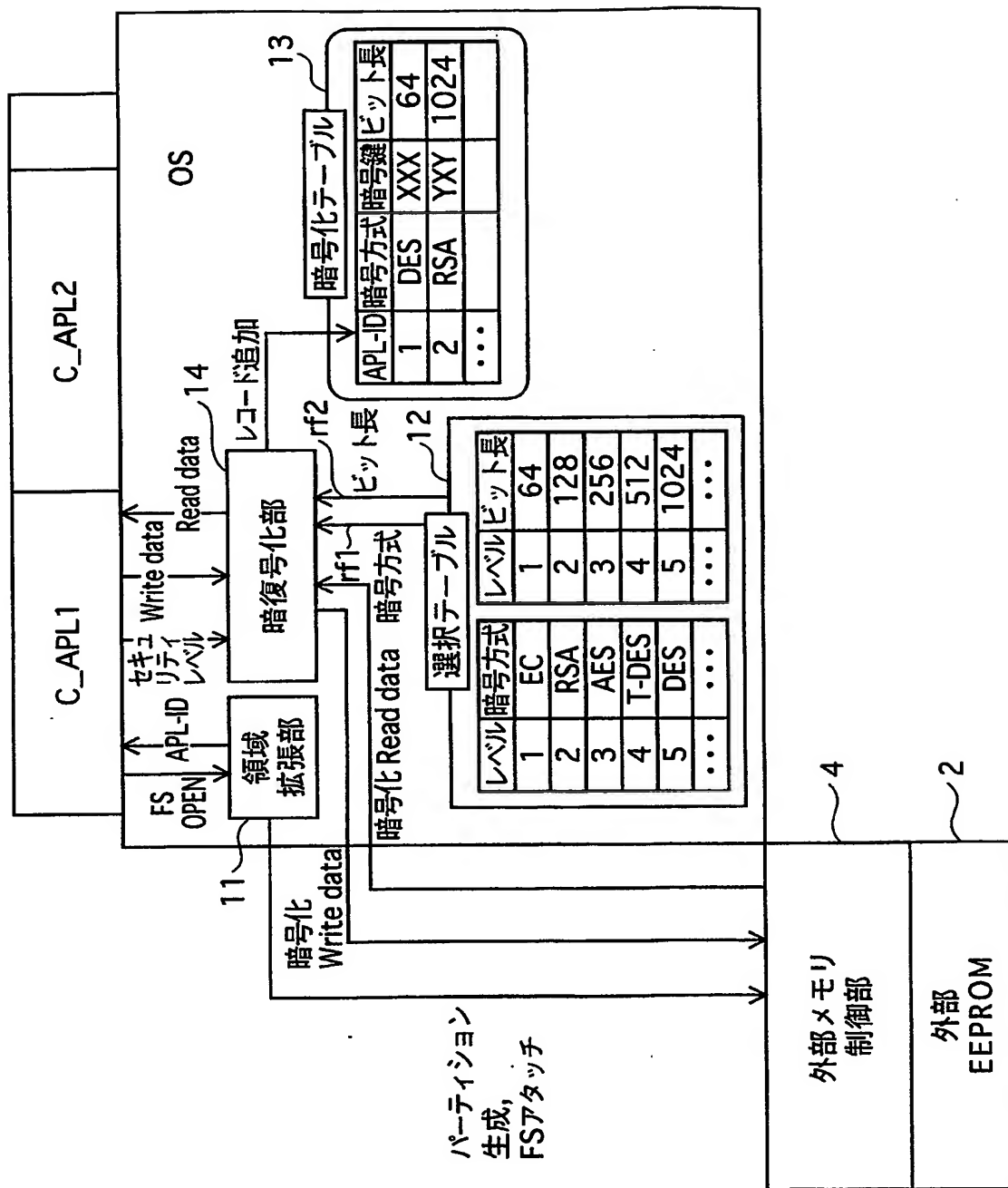
【図9】



【図 10】

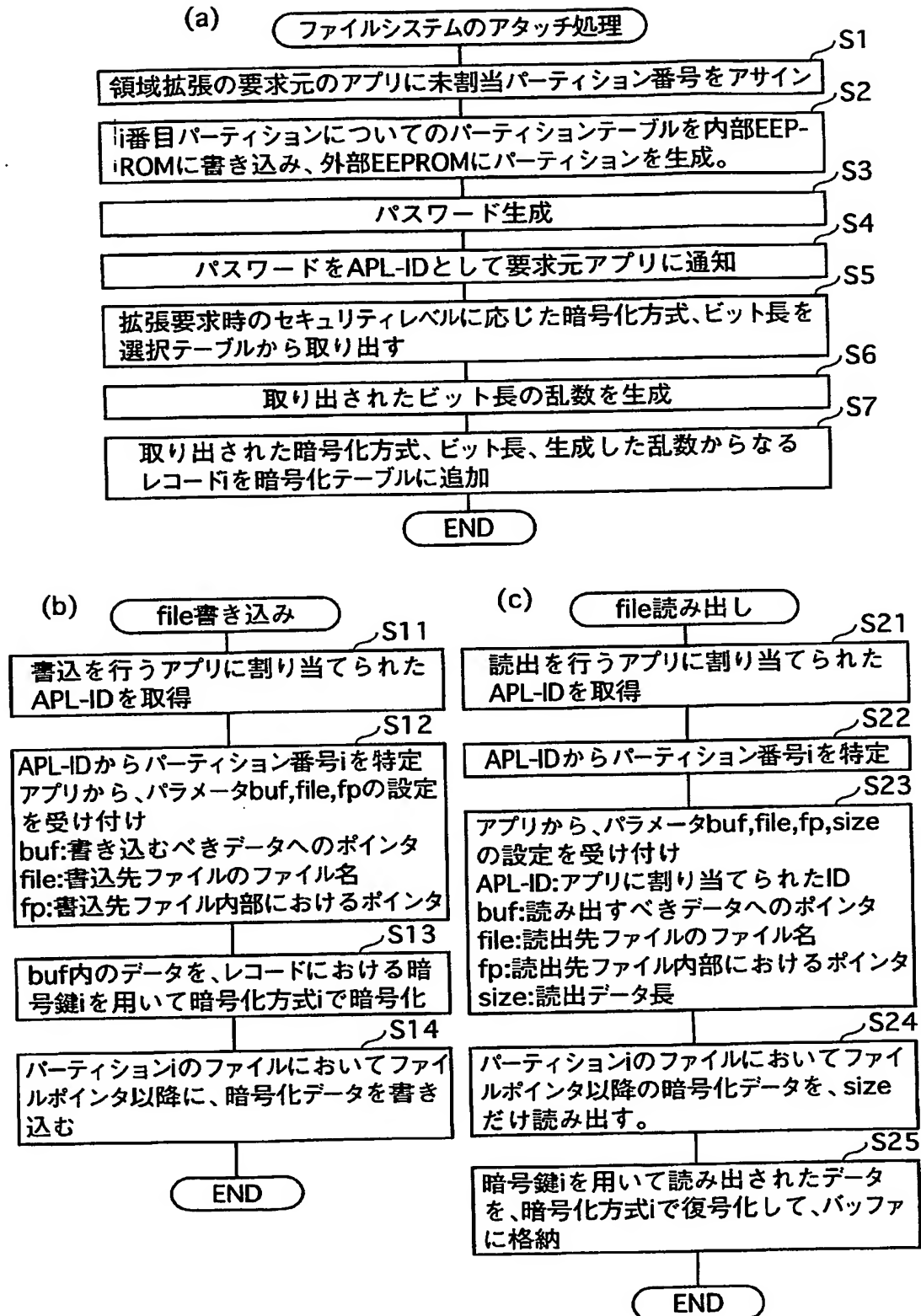


【図 11】

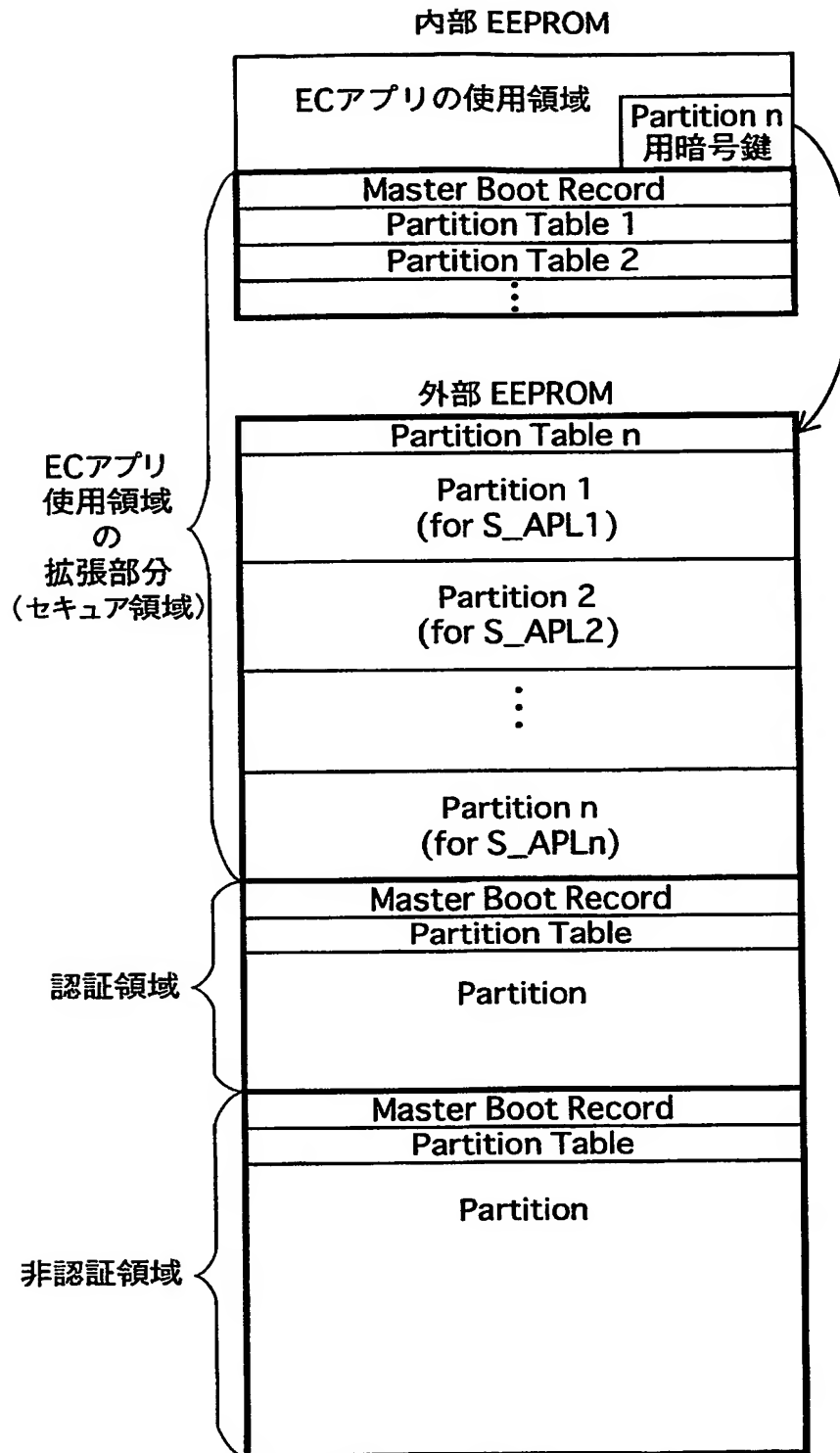


パーティション
生成,
FSアタッチ

【図12】



【図 13】



【書類名】 要約書

【課題】 ECアプリがデータを書き込もうとする際、容量が不足することのない半導体メモリカードを提供する。

【解決手段】 TRM 1 内部のEEPROM 3 にあるECアプリの使用領域を拡張する。この拡張は、内部EEPROM 3 内にパーティションテーブルを配置しつつ、TRM 1 外部EEPROM 2 にパーティションを生成してECアプリに割り当てるというものである。パーティションテーブルがTRM 1 内にあるので、生成されたパーティションテーブルは、TRM 1 内のCPU 7 からしかアクセスできない。拡張領域に対するアクセスが、TRM 1 内のCPU 7 に限られるので、格納内容の守秘性が高まる。

【選択図】 図 3

特願 2 0 0 3 - 0 2 4 1 6 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.